United States Court of Appeals

For the Eighth Circuit

No. 16-3976

United States of America

Plaintiff - Appellant

v.

Steven Shane Horton

Defendant - Appellee

Electronic Frontier Foundation

Amicus on Behalf of Appellee(s)

No. 16-3982

United States of America

Plaintiff - Appellant

v.

Beau Brandon Croghan

Defendant - Appellee

Electronic Frontier Foundation

Amicus on Behalf of Appellee(s)

Appeals from United States District Court
for the Southern District of Iowa - Council Bluffs

Submitted: April 6, 2017
Filed: July 24, 2017

Before SMITH, Chief Judge, SHEPHERD, Circuit Judge, and FENNER, District Judge.[1]

SMITH, Chief Judge.

Steven Horton and Beau Croghan were indicted separately for accessing child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). Both men moved to suppress evidence obtained through a warrant authorizing a search of their respective computers through the use of a Network Investigative Technique (NIT). In a combined order, the district court granted suppression. The government appeals pursuant to 18 U.S.C. § 3731. We reverse.

I. *Background*

The Onion Router ("Tor") network exists to provide anonymity to Internet users by masking user data, hiding information by funneling it through a series of interconnected computers. The Tor Project, a not-for-profit research organization in

[1]The Honorable Gary A. Fenner, United States District Judge for the Western District of Missouri, sitting by designation.

Massachusetts, provides free downloads of the Tor program on its website. Although Tor's intended users include whistleblowers, journalists, law enforcement personnel, activists, and privacy-minded consumers, users with more nefarious motives have used Tor's anonymity capabilities for criminal purposes.

In September 2014, the FBI began investigating an internet forum for sharing child pornography hosted on the Tor network called "Playpen." Accessible through a web address of seemingly random letters and numbers, users entered Playpen by creating a username and password. Playpen had more than 150,000 registered accounts. In January 2015, FBI agents gained access to Playpen servers and relocated the website content to servers in a secure government facility in the Eastern District of Virginia. The agents assumed administrative control of the site. Although FBI investigators could monitor Playpen traffic, users were still cloaked by the Tor encryption technology.

On February 20, 2015, FBI Special Agent Douglas Macfarlane, a 19-year veteran of the agency, applied for a warrant in the Eastern District of Virginia to search computers that accessed Playpen. The warrant described the application of the NIT, which sent computer code to Playpen users' computers that instructed the computers to transmit certain information back to the government. The information sent back included the computer's Internet Protocol (IP) address, operating system information, operating system username, and its Media Access Control (MAC) address, which is a unique number assigned to each network modem. Although Playpen was hosted in the Eastern District of Virginia, the warrant explained that "the NIT may cause [a defendant's] computer—wherever located—to send to a computer controlled by or known to the government, network level messages containing information that may assist in identifying the computer." A United States magistrate judge signed the warrant, and the FBI began collecting the personal data of Playpen users.

During the warrant period, Horton accessed Playpen with the username "boybuttlover123." The FBI located Horton in the Southern District of Iowa through information obtained by the NIT. Horton was arrested and charged in Iowa. Croghan also accessed Playpen during the relevant time period, using the username "beau2358." Through the NIT, law enforcement located his home in Iowa, executed a search of his home, and indicted him. Both Horton and Croghan moved to suppress evidence obtained through the NIT. In a combined order, the district court found that the magistrate judge exceeded her statutory authority by issuing the NIT warrant beyond the district court's jurisdictional boundaries. *See* Fed. R. Crim. P. 41(b). The district court noted that "a warrant issued without proper jurisdiction is void *ab initio* and . . . any search conducted pursuant to such warrant is the equivalent of a warrantless search." *United States v. Croghan*, 209 F. Supp. 3d 1080, 1090 (S.D. Iowa 2016). The district court suppressed the evidence obtained through the warrant. *Id.* at 1091.

This single NIT warrant executed in Virginia has implicated more than a hundred defendants across the United States. More than 40 district courts have held hearings regarding suppression of evidence generated from the NIT, including several courts in this circuit. *See, e.g.*, *United States v. Dzwonczyk*, No. 4:15-CR-3134, 2016 WL 7428390 (D. Neb. Dec. 23, 2016); *United States v. Johnson*, No. 15-00340-01-CR-W-GAF, 2016 WL 6136586 (W.D. Mo. Oct. 20, 2016); *United States v. Jean*, 207 F. Supp. 3d 920 (W.D. Ark. 2016); *see also United States v. Taylor*, No. 2:16-CR-00203-KOB-JEO-1, 2017 WL 1437511, at *3–4 (N.D. Ala. Apr. 24, 2017) (collecting cases). Most district courts that have addressed these suppression motions have denied them, but they have taken varying approaches in reaching that result. *See Dzwonczyk*, 2016 WL 7428390, at *4 ("[T]he Court takes a different path to this [non-suppression] result."). Only a few have granted suppression, and all used similar reasoning. *See, e.g.*, *United States v. Workman*, 205 F. Supp. 3d 1256 (D. Colo. 2016); *United States v. Levin*, 186 F. Supp. 3d 26 (D. Mass. 2016); *United States v. Arterbury*, No. 15-CR-182-JHP, 2016 U.S. Dist.

LEXIS 67091 (N.D. Okla. Apr. 25, 2016), *adopted by* No. 15–CR–182–JHP, 2016 U.S. Dist. LEXIS 67092 (N.D. Okla. May 17, 2016).

II. *Discussion*

"On appeal from a grant of a motion to suppress, we review a district court's findings of fact for clear error and its legal conclusions de novo." *United States v. Marasco*, 487 F.3d 543, 547 (8th Cir. 2007). We will affirm the district court's decision "unless it is not supported by substantial evidence on the record; it reflects an erroneous view of the applicable law; or upon review of the entire record, the appellate court is left with the definite and firm conviction that a mistake has been made." *United States v. Layne*, 973 F.2d 1417, 1420 (8th Cir. 1992). This appeal challenges the lower court's legal conclusions, so our review is de novo.

A. *The Fourth Amendment*

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. "[W]hat [a citizen] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Katz v. United States*, 389 U.S. 347, 351 (1967). "The fact that the electronic device employed to achieve [the search] did not happen to penetrate the [defendant's physical space] can have no constitutional significance." *See id.* at 353.

We first address whether a warrant was required for the use of a NIT. At least one district court in this circuit has determined that a warrant would likely be unnecessary for an NIT that exclusively searched for IP addresses, relying on a line of cases allowing third-party subpoenas of the same. *See Jean*, 207 F. Supp. 3d at 933 ("IP addresses are unlikely to be entitled to the same Fourth Amendment protections

as are the substantive contents of users' computers."). A defendant's publicly available information may not be entitled to Fourth Amendment protection. *See Katz*, 389 U.S. at 351 ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."). But, "[t]he government is not permitted to conduct a warrantless search of a place in which a defendant has a reasonable expectation of privacy simply because it intends to seize property for which the defendant does not have a reasonable expectation of privacy." *Workman*, 205 F. Supp. 3d at 1265.

This case differs from cases in which an IP address is voluntarily provided to third parties. *See United States v. Christie*, 624 F.3d 558, 573 (3d Cir. 2010) ("Federal courts have uniformly held that 'subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation' because it is voluntarily conveyed to third parties." (quoting *United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008))). In this case, the FBI sent computer code to the defendants' respective computers that searched those computers for specific information and sent that information back to law enforcement. Even if a defendant has no reasonable expectation of privacy in his IP address, he has a reasonable expectation of privacy in the contents of his personal computer. *See United States v. Turner*, 839 F.3d 429, 434 (5th Cir. 2016) (saying "a privacy interest exists in the electronic contents of computers and cell phones"). Moreover, the NIT retrieved content from the defendants' computers beyond their IP addresses. We conclude the execution of the NIT in this case required a warrant. "Our answer to the question of what police must do before searching a [computerized device] . . . is accordingly simple—get a warrant." *Riley v. California*, 134 S. Ct. 2473, 2495 (2014).

B. *Magistrate Jurisdiction*

Congress provided judicial authority to United States magistrate judges "within the district in which sessions are held by the court that appointed the magistrate judge . . . and elsewhere as authorized by law." 28 U.S.C. § 636(a). This authority

may be modified by the Rules of Criminal Procedure. *Id.* § 636(a)(1). When the NIT warrant was issued in this case, Federal Rule of Criminal Procedure 41 authorized a magistrate judge "to issue a warrant to search for and seize a person or property located within the district." Fed. R. Crim. P. 41(b)(1). The Rule provided exceptions to this jurisdictional limitation for property moved outside of the jurisdiction, for domestic and international terrorism, for the installation of a tracking device, and for property located outside of a federal district. *See id.*[2] None of these exceptions expressly allow a magistrate judge in one jurisdiction to authorize the search of a computer in a different jurisdiction.

The government argues that the tracking-device exception in Rule 41(b)(4) should apply here. This exception authorizes the magistrate judge "to issue a warrant to install within the district a tracking device," *see id.*, using "an electronic or mechanical device which permits the tracking of the movement of a person or object," 18 U.S.C. § 3117(b). The government argues that the defendants made a "virtual" trip

---

[2]On December 1, 2016, Federal Rule of Criminal Procedure 41(b)(6) was added to provide an additional exception to the magistrate's jurisdictional limitation by allowing warrants for programs like the NIT:

> a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:
>
> > (A) the district where the media or information is located has been concealed through technological means; or
> >
> > (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

to the Eastern District of Virginia to access child pornography and that investigators "installed" the NIT within that district. Although plausible, this argument is belied by how the NIT actually worked: it was installed on the defendants' computers in their homes in Iowa. The government rightly points out that our court interprets Rule 41 flexibly in light of advances in technology, *see United States v. N.Y. Tel. Co.*, 434 U.S. 159, 169 (1977); *United States v. Falls*, 34 F.3d 674, 678–79 (8th Cir. 1994), but we agree with the district court that the "virtual trip" fiction "stretches the rule too far," *Croghan*, 209 F. Supp. 3d at 1088 (quoting *United States v. Michaud*, No. 3:15-CR-05351-RJB, 2016 WL 337263, at *6 (W.D. Wash. Jan. 28, 2016)). We agree with the majority of courts that have reviewed the NIT warrant. These courts have concluded that "the plain language of Rule 41 and the statutory definition of 'tracking device' do not . . . support so broad a reading as to encompass the mechanism of the NIT used in this case." *Id.* Thus, we hold that the NIT warrant exceeded the magistrate judge's jurisdiction.

C. *Rule 41 Violation*

Once we have determined that Rule 41 has been violated, we next consider whether the violation was merely technical or instead rises to the level of a violation of the Fourth Amendment. *United States v. Krueger*, 809 F.3d 1109, 1113 (10th Cir. 2015); *United States v. Moore*, 41 F.3d 370, 375 (8th Cir. 1994) (analyzing whether a warrant defect was substantive or "a mere technical" error). A Rule 41 violation "is not per se an unreasonable search and seizure in violation of the Fourth Amendment." *United States v. Welch*, 811 F.3d 275, 280 (8th Cir.), *cert. denied*, 136 S. Ct. 2476 (2016). "Absent a constitutional infirmity, the exclusionary rule is applied only to violations of Federal Rule 41 that prejudice a defendant or show reckless disregard of proper procedure." *United States v. Hyten*, 5 F.3d 1154, 1157 (8th Cir. 1993). Thus, we need not address prejudice or reckless disregard for procedure if we determine that a warrant issued outside of a magistrate's jurisdictional boundaries is a violation of constitutional magnitude—that is, a violation of the Fourth Amendment.

On this question, the district court determined that "because 'the magistrate judge lacked authority, and thus jurisdiction, to issue the NIT Warrant, there simply was no judicial approval' of the NIT Warrant as required by the Fourth Amendment." *Croghan*, 209 F. Supp. 3d at 1090 (quoting *Levin*, 186 F. Supp. 3d at 36). The court "adopt[ed] the well-reasoned decisions in *Levin* and *Arterbury* and conclude[d] that a warrant issued without proper jurisdiction is void *ab initio* and that any search conducted pursuant to such warrant is the equivalent of a warrantless search." *Id.* Most district courts have determined that the Rule 41 violation here does not violate the Constitution. Our sister circuits, however, have concluded otherwise.

In *United States v. Glover*, the D.C. Circuit rejected a warrant that authorized the installation of an audio recording device in a defendant's vehicle, "regardless of whether the vehicle was located in the District of Columbia, District of Maryland, or the Eastern District of Virginia." 736 F.3d 509, 510 (D.C. Cir. 2013). Relevant to this case, the court held that the warrant "appears, on its face, to be in violation" of Rule 41. *Id.* at 515. "Even if we assume that an imperfect authorizing order could be thought facially sufficient, we do not see how a blatant disregard of a district judge's jurisdictional limitation can be regarded as only 'technical.'" *Id.* The court reversed the lower court and ordered a new trial, suppressing the evidence obtained from the "facially insufficient" warrant. *Id.* at 510.

In *United States v. Krueger*, the Tenth Circuit determined that a similar Rule 41 violation prejudiced the defendant, without reaching the constitutional question of magistrate jurisdiction. 809 F.3d at 1116–17. Then-Judge Gorsuch explained separately in a concurrence that he believed jurisdictional errors under Rule 41 were errors of constitutional magnitude:

> For looking to the common law at the time of the framing it becomes quickly obvious that a warrant issued for a search or seizure beyond the territorial jurisdiction of a magistrate's powers under positive law was

> treated as no warrant at all—as *ultra vires* and *void ab initio* to use some of the law's favorite Latin phrases—as null and void without regard to potential questions of "harmlessness" (such as, say, whether another judge in the appropriate jurisdiction would have issued the same warrant if asked). . . . The principle animating the common law at the time of the Fourth Amendment's framing was clear: a warrant may travel only so far as the power of its issuing official. And that principle seems clearly applicable—and dispositive—here.

Id. at 1123–24 (Gorsuch, J., concurring).

The district court followed this logic, finding the NIT warrant invalid at its inception and therefore the constitutional equivalent of a warrantless search. *Croghan*, 209 F. Supp. 3d at 1090–91; *see also Taylor*, 2017 WL 1437511, at *14 ("[T]he Fourth Amendment does not impose a venue requirement . . . . But inherent in the notion of a 'neutral, detached magistrate' is that the magistrate have authority to issue the warrant." (citation omitted)). In response, the government argues that because the NIT warrant was proper in the Eastern District of Virginia, it cannot be wholly void or void *ab initio*. *See United States v. Ryan Anthony Adams*, No. 6:16-CR-11-ORL-40GJK, 2016 WL 4212079, at *6 (M.D. Fla. Aug. 10, 2016) ("The Court finds that the magistrate judge in the Eastern District of Virginia had the authority to issue search warrants—that is, the inherent power to do so."). The possibility that the magistrate could have executed a proper warrant in the Eastern District of Virginia, however, does not save this warrant from its jurisdictional error. *See Glover*, 736 F.3d at 510 (rejecting a warrant for multiple jurisdictions including the magistrate's proper district); *United States v. Master*, 614 F.3d 236, 241 (6th Cir. 2010) (rejecting a warrant issued by a magistrate with warrant-issuing authority in a neighboring county); *see also Krueger*, 809 F.3d at 1116 (rejecting the argument of warrant validity "so long as the Government hypothetically could have obtained the warrant from a different federal magistrate judge with warrant-issuing authority under

the Rule"). We agree with the district court and find that the NIT warrant was void *ab initio*, rising to the level of a constitutional infirmity.[3]

D. *Good-Faith Exception*

"The fact that a Fourth Amendment violation occurred—*i.e.*, that a search or arrest was unreasonable—does not necessarily mean that the exclusionary rule applies." *Herring v. United States*, 555 U.S. 135, 140 (2009). "Even when an unreasonable search does exist, the Supreme Court has explained, we must be persuaded that 'appreciable deterrence' of police misconduct can be had before choosing suppression as the right remedy for a Fourth Amendment violation." *Krueger*, 809 F.3d at 1125 (Gorsuch, J., concurring) (quoting *Herring*, 555 U.S. at 141). A warrantless search is "presumptively unreasonable and suppression is an appropriate remedy unless the *Leon* good faith exception applies." *Croghan*, 209 F. Supp. 3d at 1090–91; *see United States v. Leon*, 468 U.S. 897 (1984). We review the application of the *Leon* exception de novo. *United States v. Houston*, 665 F.3d 991, 994 (8th Cir. 2012).

"The Fourth Amendment contains no provision expressly precluding the use of evidence obtained in violation of its commands, and an examination of its origin and purposes makes clear that the use of fruits of a past unlawful search or seizure 'work[s] no new Fourth Amendment wrong.'" *Leon*, 468 U.S. at 906 (alteration in original) (quoting *United States v. Calandra*, 414 U.S. 338, 354 (1974)). In *Leon*, the Supreme Court determined that "the marginal or nonexistent benefits produced by suppressing evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial costs of exclusion." *Id.* at 922. In analyzing this good-faith exception in the context of the NIT warrant, the

[3]The defendants and Amicus Curiae argue that the NIT warrant failed to meet the Fourth Amendment's particularity requirement. Because we find that the NIT warrant failed to meet constitutional standards on alternative grounds, we decline to address this issue.

district court determined "that *Leon* is inapplicable to issuance of the NIT Warrant because the NIT Warrant was issued without jurisdiction and was, therefore, void *ab initio*." *Croghan*, 209 F. Supp. 3d at 1091. In making this determination, the district court relied heavily on the reasoning in *Levin*:

> To hold that the good-faith exception is applicable here would collapse the distinction between a voidable and a void warrant. But this distinction is meaningful: the former involves "judicial error," such as "misjudging the sufficiency of the evidence or the warrant application's fulfillment of the statutory requirements[,]" while the latter involves "judicial *authority*," *i.e.*, a judge "act[ing] outside of the law, outside of the authority granted to judges in the first place."

Levin, 186 F. Supp. 3d at 41 (alterations in original) (quoting *State v. Hess*, 770 N.W.2d 769, 776 (Wis. Ct. App. 2009)). The government argues that this distinction between "voidable" and "void" warrants is untenable in the good-faith exception context, and we agree.

In *Master*, the Sixth Circuit analyzed a case in which a state judge issued a warrant for a search outside of his jurisdictional boundaries that he "had no authority to issue." 614 F.3d at 241. The court expressly rejected an argument that when a judge "lack[s] legal authority to issue the relevant warrant, the good faith exception is foreclosed." *Id.* Because of intervening Supreme Court precedent, the court abrogated a previous holding in which the court did not apply the *Leon* exception to a warrant void *ab initio*. *See id.* at 241–43 (overruling in part *United States v. Scott*, 260 F.3d 512 (6th Cir. 2001)). "Arguably, the issuing magistrate's lack of authority has no impact on police misconduct . . . ." *Id.* at 242. Our review of relevant Supreme Court precedent leads us to a similar conclusion: that the *Leon* exception can apply to warrants void *ab initio* like this one.

In *Leon*, the Supreme Court noted that "[p]enalizing the officer for the magistrate's error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations." 468 U.S. at 921. The Court has applied the *Leon* exception in a strikingly wide array of cases. *See, e.g.*, *Davis v. United States*, 564 U.S. 229 (2011) (binding precedent overruled); *Herring*, 555 U.S. 135 (recalled warrant); *Hudson v. Michigan*, 547 U.S. 586 (2006) (knock-and-announce violation); *Arizona v. Evans*, 514 U.S. 1 (1995) (outdated arrest warrant); *Illinois v. Krull*, 480 U.S. 340 (1987) (reliance on an unconstitutional statute). In all these cases, the Court has not focused on the type of Fourth Amendment violation at issue, but rather confined the "'good-faith inquiry . . . to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal' in light of 'all of the circumstances.'" *Herring*, 555 U.S. at 145 (quoting *Leon*, 468 U.S. at 922 n.23). "As laid out in our cases, the exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Id.* at 144. We agree with the Sixth Circuit that regardless of the type of warrant at issue that "[t]he Supreme Court has effectively created a balancing test by requiring that in order for a court to suppress evidence following the finding of a Fourth Amendment violation, 'the benefits of deterrence must outweigh the costs.'" *Master*, 614 F.3d at 243 (quoting *Herring*, 555 U.S. at 141).

Having determined that the *Leon* exception may apply to a warrant void *ab initio*, the question remains whether it should apply here. "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Herring*, 555 U.S. at 144. "As with any remedial device, the rule's application has been restricted to those instances where its remedial objectives are thought most efficaciously served." *Arizona*, 514 U.S. at 11. "Suppression of evidence . . . has always been our last resort, not our first impulse." *Hudson*, 547 U.S. at 591. In this case, the district court found that because "law enforcement was sufficiently experienced, and that there existed adequate case law casting doubt on

magisterial authority to issue precisely this type of NIT Warrant . . . the good faith exception is inapplicable." *Croghan*, 209 F. Supp. 3d at 1093. We disagree.

Because *Leon* provides an exception for good faith, we apply it as long as the circumstances do not demonstrate bad faith, such as:

> (1) when the affidavit or testimony supporting the warrant contained a false statement made knowingly and intentionally or with reckless disregard for its truth, thus misleading the issuing judge; (2) when the issuing judge "wholly abandoned his judicial role" in issuing the warrant; (3) when the affidavit in support of the warrant is "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable"; and (4) when the warrant is "so facially deficient" that no police officer could reasonably presume the warrant to be valid.

Houston, 665 F.3d at 995 (quoting *United States v. Proell*, 485 F.3d 427, 431 (8th Cir. 2007)).

The defendants argue that the NIT warrant demonstrates such bad faith. The defendants argue that the NIT warrant affidavit exhibited a reckless disregard for its truth by listing the Eastern District of Virginia as the place to be searched, when law enforcement knew that computers could be searched anywhere in the country. At least one court has agreed with this reasoning. *See Workman*, 205 F. Supp. 3d at 1264 ("In my view, had [the magistrate judge] understood that the NIT technology would search computers in other districts—rather than track information as it traveled from her district to others—she probably would not have issued the NIT Warrant given the limitations of the Rule."). The warrant, however, discusses at length the NIT and how it would be used to connect to computers "wherever located." Even if it were misleading to label the place to be searched as the Eastern District of Virginia, a reasonable reader would have understood that the search would extend beyond the

boundaries of the district because of the thorough explanation provided in the attached affidavit. This does not amount to a reckless disregard for the truth.

The defendants also argue that the NIT warrant was facially deficient because FBI agents should have known that a warrant purporting to authorize thousands of searches throughout the country could not be valid. Specifically, Horton argues that "there can be no credible argument that officers reasonably believed that none of the 214,898 members of [Playpen] were located outside of Virginia." *E.g.*, *In re Warrant to Search a Target Compt. at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013) (finding a similar warrant that exceeded the territorial limits of Rule 41 invalid). We, however, will not find an obvious deficiency in a warrant that a number of district courts have ruled to be facially valid. *See, e.g.*, *Johnson*, 2016 WL 6136586, at *5; *Jean*, 207 F. Supp. 3d at 943. Further, we have declined to impose an obligation on law enforcement to "know the legal and jurisdictional limits of a judge's power to issue interstate search warrants." *Houston*, 665 F.3d at 996. Law enforcement did not demonstrate bad faith, and we will apply the *Leon* balancing test as instructed by the Supreme Court.[4]

"For exclusion to be appropriate, the deterrence benefits of suppression must outweigh its heavy costs." *Davis*, 564 U.S. at 237. Because Rule 41 has been updated to authorize warrants exactly like this one, there is no need to deter law enforcement from seeking similar warrants. As noted above, we do not believe that law enforcement acted in bad faith, and "[e]xclusion of the evidence seized pursuant to the NIT warrant would serve little deterrent purpose where the mistaken conduct of the magistrate judge, not the officers, invalidated the warrant." *Taylor*, 2017 WL 1437511, at *16. And the costs of exclusion in this case are substantial. Suppression

[4]Additionally, the defendants argue that the FBI's sting operation itself was unreasonable, but this issue has no bearing on whether law enforcement acted reasonably by obtaining and relying on the NIT warrant. Thus, we will not address this issue.

here would extend beyond the present defendants and impact multiple cases within this circuit. On balance, the marginal benefit of deterrence fails to outweigh the associated costs: "letting guilty and possibly dangerous defendants go free—something that 'offends basic concepts of the criminal justice system.'" *Herring*, 555 U.S. at 141 (quoting *Leon*, 468 U.S. at 908). We therefore apply the *Leon* exception to this case and reverse the district court's grant of suppression.

III. *Conclusion*

Accordingly, we reverse the district court's order suppressing the evidence and remand these cases for further proceedings.

FENNER, District Judge, concurring in part and dissenting in part.

I respectfully dissent from Parts II.B and II.C of the court's opinion. Under Federal Rule of Criminal Procedure 41(b)(4), a magistrate judge is authorized to issue a warrant to install a tracking device within the magistrate's district regardless of whether the movement of the person or property being tracked moves outside of the district. Fed. R. Crim. P. 41(b)(4). As the majority acknowledged, Rule 41 is interpreted with flexibility in light of advances of technology. *See United States v. New York Tel. Co.*, 434 U.S. 159 (1977); *United States v. Falls*, 34 F.3d 674 (8th Cir. 1994). I believe the "installation" of the tracking device occurred where law enforcement attached the NIT to the flow of information, *i.e.* the Eastern District of Virginia. *See United States v. Jean*, 207 F. Supp. 3d 920, 942-43 (W.D. Ark. 2016) (reasoning that installation occurred in the Eastern District of Virginia because the NIT was designed to track the flow of intangible property and law enforcement did not leave the jurisdiction to attach the NIT to the defendant's computer). Given the flexibility with which Rule 41 is interpreted and the facts of this case, I would conclude that Rule 41 does encompass the NIT warrant and find no violation of Rule 41. I concur in the court's opinion in all other respects.
